SELECT SPECIAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT REVIEW COMMITTEE

THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

LOOKING AHEAD: A DISCUSSION GUIDE

MARCH 2002

The Select Special Freedom of Information and Protection of Privacy Act Review Committee

Brent Rathgeber, Q.C., MLA Edmonton-Calder, Chair
Mary Anne Jablonski, MLA Red Deer-North, Deputy Chair
Debby Carlson, MLA Edmonton-Ellerslie
Alana DeLong, MLA Calgary-Bow
Broyce Jacobs, MLA Cardston-Taber-Warner
Thomas Lukaszuk, MLA Edmonton-Castle Downs
Hugh MacDonald, MLA Edmonton-Gold Bar
Brian Mason, MLA Edmonton-Highlands
Gary Masyk, MLA Edmonton-Norwood

Please send your comments to:

Corinne Dacyshyn, Committee Clerk
Legislative Assembly of Alberta
801 Legislature Annex
9718 – 107 Street
Edmonton, Alberta T5K 1E4
FAX: (780) 427-5688
TEL: (780) 427-1348
e-mail corinne.dacyshyn@assembly.ab.ca

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act* (often referred to as the *FOIP Act*) was given Royal Assent in 1994 and came into force for the Government of Alberta on October 1, 1995. Coverage was extended to local public bodies in stages – to school jurisdictions on September 1, 1998; to health care bodies on October 1, 1998; to post-secondary institutions on January 4, 1999; and to local government bodies on October 1, 1999. The *Act* now applies to approximately 1500 public bodies. It demonstrates to Albertans the commitment to open, accessible and accountable government and protection of the privacy of Albertans.

In 1998, a Select Special FOIP Act Review Committee conducted the first review of the *Act*. The 1998 review resulted in a comprehensive *FOIP Amendment Act, 1999*, including several dozen changes to the original *Act.* The Committee recommended that a second review be conducted within three years (**section 97**) to allow local public bodies, in particular, an opportunity to provide further recommendations once they all had more experience in administering the *Act.*

Since the last review of the *Act*, there have been some significant developments on the access and privacy landscape.

- All the sectors that were to be covered by the *FOIP Act* were subject to the *Act* by October 1999.
- The Alberta *Health Information Act* and regulations came into force on April 25, 2001. Health care bodies that are subject to the *FOIP Act* continue to follow the *FOIP Act* for non-health information, but now follow the *Health Information Act* for health information.
- Canada's *Personal Information Protection and Electronic Documents Act* came into force on January 1, 2001. This requires private sector organizations to comply with privacy rules. That *Act* has applied to federally regulated organizations, such as banks, since 2001, and will apply to all private-sector organizations unless equivalent provincial legislation is in place by 2004.

In addition, there are other key factors that influence access and privacy legislation, such as the rapid development and sophistication of information technology, the ability to access government services electronically and, in some cases, heightened concerns about public security.

In the present review, the Committee will focus upon:

- Whether the *Act* and its supporting policy and administration provides an appropriate balance of access to information and protection of privacy, in accordance with the original intent;
- The implications to all sectors subject to the *Act* and/or any expansion of the *Act* to include other sectors; and
- The impact of accessing government services electronically and the growth and sophistication of existing and emerging information technologies on privacy.

The review does not include:

- Access and privacy issues relating to individual health information within the scope of the *Health Information Act*; and
- Privacy protection in the private sector as a result of the passage of the federal *Personal Information Protection and Electronic Documents Act.*

Your views are important to us to ensure that a proper balance between providing access to information and protecting individual privacy is maintained. This discussion guide was developed to help you contribute to this important exercise.

Your submission may be sent by facsimile or e-mail. If sending e-mail, please include your mailing address to receive a copy of the Committee's reports. Where possible, submissions should be signed. Anonymous submissions will not be considered. A questionnaire is included as an appendix to assist you with your response. Other forms of written submission are also welcome. All submissions should be received by **May 10, 2002.**

Please send your comments to:

Corinne Dacyshyn
Committee Clerk
Legislative Assembly of Alberta
801 Legislature Annex
9718 – 107th Street
Edmonton, Alberta T5K 1E4
FAX: (780) 427-5688
TEL: (780) 427-1348
e-mail: corinne.dacyshyn@assembly.ab.ca

Please note that submissions will be publicly available in the Legislature Library. Do not include any personal or confidential business information that you do not want to be made available to the public.

The Select Special Freedom of Information and Protection of Privacy Act Review Committee will consider your input in the preparation of its recommendations. The Committee's report will be provided to the Legislative Assembly in Fall 2002. It will include a list of respondents.

Note: All sections of the *Act* referenced in this document are from the *Freedom of Information and Protection of Privacy (FOIP) Act,* RSA 2000, Chapter F-25. If you wish to cite sections of the *FOIP Act*, please ensure that you cite current section numbers, as they appear in RSA 2000.

FUNDAMENTAL PRINCIPLES

There are five fundamental principles that provide the building blocks upon which the *Act* is based. These are:

1) To allow any person a right of access to the records in the custody or under the control of a public body subject only to limited and specific exceptions;

2) To control the manner in which a public body may collect personal information from individual Albertans; to control the use the public body may make of that information; and to control the disclosure by a public body of such information;

3) To allow individuals, subject to limited and specific exceptions, the right to have access to information about themselves held by a public body;

4) To allow individuals the right to request corrections to personal information about themselves held by a public body; and

5) To provide for an independent review of decisions made by public bodies under the legislation and the resolution of complaints.

Question

1. Are the fundamental principles of the legislation appropriate? If not, please explain why and make suggestions for improvement.

THE SCOPE OF THE ACT

The *Act* currently applies to:

- a department, branch or office of the Government of Alberta,
- an agency, board, commission, corporation, office or other body designated as a public body in the regulations,
- the Executive Council Office,
- the office of a member of Executive Council,
- the Legislative Assembly Office,
- the office of the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner or the Information and Privacy Commissioner,
- educational bodies including post-secondary educational institutions, school boards and charter schools,
- health care bodies including regional health authorities, the Alberta Mental Health Board and the Alberta Cancer Board, and
- local government bodies including municipalities, police services and commissions, Metis settlements, irrigation and drainage districts, housing management bodies and public libraries.

Criteria for Inclusion

The FOIP legislation applies to a number of organizations that are affiliated with government. Provincial government agencies, boards and commissions are made subject to the *Act* by including them in Schedule 1 of the *FOIP Regulation*. The criteria for inclusion in the Schedule are that the Government of Alberta:

- appoints a majority of the members to the body or the governing body of the organization;
- provides a majority of the organization's funding; or
- for a corporation, has a controlling interest in its share capital.

Organizations affiliated with local government are not listed individually. They are included if they fall within a definition in the *Act* (**section 1(i)(xii)**) which says that an organization is a local government body if:

- it is created or owned by a local public body, and
- all of the members or officers are appointed or chosen by that body.

In both cases, the criteria for inclusion within the scope of the *Act* are based on government control through power of appointment or financial interest. This has been called a *structural* approach, requiring accountability to taxpayers for organizations within the control of government.

There are, however, many types of organizations that have an increasingly significant role in the implementation of government policy, but which do not meet these criteria. These include private-sector organizations whose primary function is to perform some regulatory function, such as inspections and licensing, or to act as a professional accreditation or disciplinary body.

A *functional* approach to inclusion within access and privacy legislation assumes that organizations that perform a regulatory function should have some of the same obligations as government.

Question

2. Are the current criteria (structural approach) for including organizations within the scope of the *Act* appropriate? Do these criteria provide the flexibility needed for changing organizational structures or models (e.g. public-private partnerships or shared service arrangements)?

RECORDS AND INFORMATION TO WHICH THE ACT APPLIES

Section 4 of the *Act* lists certain classes of records and information to which the *FOIP Act* does not apply, e.g. court records, questions used on examinations or tests and personal or constituency records of elected members of local public bodies. Currently,

the classes of records and information listed in **section 4** are excluded from both **Part 1** of the *Act* (access to information) and **Part 2** of the *Act* (protection of privacy of personal information).

Section 5 describes the relationship between the *Act* and other legislation. The *FOIP Act* prevails over inconsistent or conflicting provisions in other legislation unless the other Act or the *FOIP Regulation* expressly provides that the other legislation prevails despite the *FOIP Act.* The purpose of these "paramountcy" provisions is to allow for access to information and the protection of personal information to be specifically set out in a separate legislative scheme, e.g. adoption records under the *Child Welfare Act.*

Questions

3. Are there any cases where excluded records or information should continue to be excluded from the access provisions of the *Act* (**Part 1**) but made subject to the *Act's* privacy provisions (**Part 2**)? Please specify which records or information and explain why this would be an improvement.
4. Are there any cases where a separate scheme of access and privacy for records or information that are not subject to the *FOIP Act* unreasonably limits access to records or the protection of personal information? Please specify which records or information and suggest how access or privacy protection might be improved.

ACCESS TO RECORDS

The Access Process

The first fundamental principle of the *Act* concerns access to records. **Sections 6** to **15.1** of the *Act* provide details on the process. Anyone may request access to a record. To obtain access to a record under the *Act*, the applicant must make a request to the public body that he or she believes has custody or control of the record. The FOIP web site contains contact information for each public body. Access requests are made on a simple form or by letter, with the applicant providing as much detail as possible about the record to enable the public body to find it. The public body has a duty to assist the applicant in accessing records.

Sometimes only a part of a record is accessible because of the specific exceptions to disclosure under the *Act*. A public body must release as much of the record as it can.

A public body must respond to a request within 30 calendar days unless the time limit is extended or the request is transferred to a more appropriate public body for response. The time limits may be extended only in particular circumstances laid out in the *Act*.

The access process established in the *Act* guides how a public body must respond to an applicant. An applicant must be told whether access will be given and, if access will be given, when and how it will be given. If access is refused, the applicant must be

given reasons for the refusal as well as the name and address of a person who can answer questions about the refusal. The applicant must also be told that he or she may request a review of the decision by the Information and Privacy Commissioner. Only in very limited cases may a public body refuse to confirm or deny the existence of a record.

Where access is to be granted, a public body must provide a copy of the record requested, if the copy can normally be reproduced and to do so will not unreasonably interfere with the public body's operations.

Questions

5. Is the process for obtaining access to records appropriate? If not, please explain and provide any suggestions for improvement.
6. Do you think that an applicant can locate the public body most able to respond to his or her request (e.g. by accessing the Government of Alberta web site and/or the FOIP web site, the Government's RITE Line, or by being referred by public body staff)?

Exceptions to Disclosure

The access to information legislation in every jurisdiction recognizes that an absolute rule of openness to all records of a public body would impair the ability of the public body to discharge its responsibilities effectively. This is reflected in Alberta's *FOIP Act* by specific and limited exceptions to the general rule of public access to information held by a public body (**sections 16** to **29**).

Most of the exceptions are discretionary, allowing a public body through its head or designated official to release or withhold information.

Mandatory Exceptions

Only five very important exceptions specify under what circumstances a public body *must* refuse access to records. These are:

- disclosure harmful to the business interests of a third party;
- disclosure harmful to personal privacy;
- disclosure harmful to law enforcement;
- Cabinet and Treasury Board confidences; and
- privileged information of a third party.

Question

7. Are the mandatory exceptions to disclosure appropriate? If not, please explain why and provide suggestions for improvement.

Discretionary Exceptions

The discretionary exceptions in the *Act* include:

- records where disclosure could reasonably be expected to threaten a person's health or safety or interfere with public safety;
- confidential evaluations;
- records where disclosure could be harmful to law enforcement matters;
- records where disclosure could be harmful to intergovernmental relations;
- local public body confidences;
- advice from officials;
- commercial information of a public body;
- testing or audit procedures and results;
- privileged information;
- information where disclosure could be harmful to heritage sites or endangered forms of life; and
- information available to the public and information to be available within 60 days.

Question

8. Are the discretionary exceptions to disclosure appropriate? If not, please explain why and provide suggestions for improvement.

Fees

Fees may be required for services provided to an applicant under the *Act* (**section 93**). Fees are established on the principle that there should be a fair sharing of costs between the applicant and the public body. Fees charged for processing FOIP requests cover only a fraction of the costs actually incurred by public bodies. The *FOIP Regulation* establishes a structure and maximum rates for charging fees under the *Act* for general and personal information that ensures consistency among public bodies.

The *FOIP Regulation* states that an applicant requesting his or her own personal information cannot be assessed a fee except for copying costs, and then only if the costs exceed $10. The *Regulation* provides for a $25 initial fee for one-time requests for information other than the applicant's personal information; a $50 initial fee for continuing requests; and additional fees where the costs of processing a request for non-personal information exceeds $150.

Basically, fees may be assessed on requests for access to general records (non-personal information) for:

- locating, retrieving and producing the records;
- computer and programming time for producing electronic records;
- preparing the records for disclosure;
- copying records for release;

- supervising the inspection of records; and
- shipping charges.

The most commonly collected fees are 25 cents per page for copies and $6.75 per quarter hour for services. There is no fee for filing an appeal with the Commissioner.

The head of the public body may waive fees, upon request, if the applicant cannot afford to pay, if it is fair to excuse payment or if the record relates to a matter of public interest, such as health or safety. The applicant may request the Information and Privacy Commissioner to review the decision of the head and either agree with the head, reduce the fee or order a refund, where appropriate.

Question

9. Does the principle of sharing the costs between the public body and the applicant strike a fair balance between access rights and the responsibilities of public bodies to use their resources for program delivery? If not, please explain why and make suggestions for improvement.

Rights of Third Parties

An applicant may request information about a third party. A third party is someone other than an applicant or a public body. The *Act* tries to strike a balance between the interests of the third party and the rights of an applicant. **Sections 30** and **31** of the *Act* provide details.

The head of a public body is required to notify the third party and provide the third party with a copy of the record if the head is considering giving access to information that may fall within the exception for third party business information or if the disclosure may be an unreasonable invasion of the third party's personal privacy. Within 20 days the third party must consent to the disclosure or make representations explaining why the disclosure should not be made. The applicant must also be given notice that third party interests may be affected.

A decision as to whether access will be given must be made within 30 days of the notice to the third party. Both the third party and the applicant are notified of the decision. If the public body proposes to disclose the record, the third party has 20 days to ask the Commissioner for a review of the decision. The applicant has 60 days to ask for a review if the public body decides not to give access to a record.

Question

10. Is an appropriate balance struck between the interests of third parties and the rights of applicants? If not, please explain why and provide suggestions for improvement.

PROTECTION OF PRIVACY

The *Act* recognizes the importance Albertans place on the privacy of information about them that may be in the hands of a public body. **Part 2** of the *Act* contains the rules surrounding the collection, use and disclosure of personal information. They are based on the fair information principles established by the Organization for Economic Cooperation and Development (OECD) that have been incorporated into the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information. These fair information principles are generally used in similar legislation across Canada.

Personal information means information about an identifiable individual (**section 1(n)**).

Collection of Personal Information

A public body can collect personal information from an individual only if the collection is expressly authorized by an Act or a regulation; it relates to law enforcement; or, it is necessary for an operating program or activity of the public body (**section 33**). The individual must normally be told the purpose of the collection, the specific legal authority for the collection and who can answer questions about the collection (**section 34(2)**).

Personal information must be collected directly from the individual except in certain specifically defined circumstances such as where the individual has consented to indirect collection, another method of collection is authorized under an Act, it is collected for the purpose of law enforcement, etc. (**section 34(1)**).

Public bodies also have a duty to ensure that reasonable security arrangements are maintained for personal information in their possession (**section 38**).

Use of Personal Information

A public body may use personal information it collects from individuals only for the purpose for which it was obtained or a consistent purpose; for another purpose with the consent of the individual; or, for purposes allowed under the disclosure provisions of the *Act* (**section 39**). A consistent purpose is one that has a reasonable and direct connection to the reason the information was collected and is necessary for an operating program or statutory duty (**section 41**).

Every reasonable effort must be made by a public body to ensure the personal information used is accurate and complete (**section 35(a)**).

It is a fundamental principle that an individual has a right of access to his or her own personal information (subject to specific and limited exceptions) and a right to request a correction of information that the individual believes may contain an error or omission. The public body must either make the correction or make a note of the request for correction on the individual's file. In either case, the public body must notify the individual of the action taken within 30 days (**section 36**).

The public body must also notify any other public body or third party to whom the personal information was disclosed in the year prior to the correction or annotation. Because of the right to request a correction and the individual's right of access to his or her own personal information, a public body must retain information it uses for at least one year after it has been used (**section 35(b)**).

Disclosure of Personal Information

Specific rules are set out in the *Act* to ensure that an individual's personal information is not disclosed beyond what is required for the proper operations of a public body, or for the legitimate interests of researchers and others.

Section 40 sets out the only situations where a public body may disclose personal information without an access request. These situations include disclosure for a consistent purpose; with the individual's consent; as authorized or required by another Act or regulation of Alberta or Canada; for complying with a court order; for complying with a law of Alberta or Canada; and, to a relative of a deceased individual.

Disclosure for research purposes is constrained by **section 42**. In addition, **section 8** of the *FOIP Regulation* sets out specific requirements that must be included in researcher agreements. The *Regulation* states that if a person fails to meet the conditions of the agreement, the agreement may be immediately cancelled and the person may be guilty of an offence under **section 92(1)** of the *FOIP Act*.

The Provincial Archives of Alberta and the archives of a public body may also disclose personal information if the personal information has been in existence for 25 years or more and disclosure would not be an unreasonable invasion of personal privacy under **section 17**; or the disclosure is in accordance with the research provisions in **section 42**. There are no restrictions on the disclosure of personal information in a record that has been in existence for 75 years or more (**section 43**).

Questions

11. Is the definition of "personal information" in the *Act* appropriate? If not, please explain why and make suggestions for improvement.
12. Are the rules in the *Act* that control the manner in which public bodies collect, use and disclose personal information sufficient to protect the privacy and security of sensitive personal information? If not, please explain why and make suggestions for improvement.

PRIVACY IN THE ELECTRONIC AGE

Advances in information and communications technology continue to have a dramatic impact on Albertans. Information technology provides the means of compiling, storing, transferring and analyzing information electronically. Communications technology allows

for the transfer of this electronic data through wired networks, telephone lines and wireless radio signals.

Developments in information and communications technology have a significant effect on both the internal operations of organizations and their relations with the public. For example, the ability to access and share information, both within the organization and with contracted service providers, has brought increases in productivity for government, public organizations and businesses. The ability of organizations to gather information and provide services electronically through web sites has provided increased convenience for individuals as citizens, clients and customers.

At the same time, this rapid pace of technological change presents challenges for privacy and for the security of personal information. Technology allows for the creation, manipulation and potential sharing of databases that contain a great deal of personal information. It also allows for the transmission of that information over the Internet, wireless networks and cellular telephones, and for its storage on devices such as personal digital assistants (e.g. palm pilots) and "smart cards."

One of the main purposes of the *FOIP Act* is to control the ways in which public bodies collect, use and disclose personal information. Technology can enhance the ability of public bodies to exercise this control; for example, through electronic controls on access to personal information in databases. These include user authentication (such as biometric authentication), encryption and electronic audits. But technology also creates some risks of intentional and unintentional breaches of personal privacy. These may result from deliberate hacking into databases or the inadvertent disclosure of personal information through the inappropriate use of e-mail systems and cell phones.

Like other governments and businesses, the Alberta government is moving towards electronic access to government services. This means that Albertans may be able to send in applications for services or complete forms through a web site. For example, at present, vehicle registration can be renewed online. In the future, a one-stop shopping approach would make it possible for people to obtain services from, and share information with, many government departments, through a single point of contact. This new model raises the possibility that government bodies may need to share personal information in new ways to deliver services.

Question

13. Are there any issues associated with existing or emerging technologies that could be addressed through amendments to the *FOIP Act*? If so, please explain.

PUBLIC SECURITY

The events of September 11, 2001 heightened public awareness of the threat to security posed by terrorism, and the need for coordinated action, including information

sharing, to protect the public. Some jurisdictions have amended their legislation to expand the powers of national security agencies – in some cases, at the expense of individual privacy.

Alberta's *FOIP Act* includes a number of provisions for protecting sensitive information. For example, **section 18(1)** allows a public body to refuse to disclose any information that would interfere with public safety. **Section 20(1)(b)** allows a public body to withhold information that could hinder the defence of Canada or any ally or harm the detection, prevention or suppression of espionage, sabotage or terrorism. **Section 21(1)** allows for non-disclosure of information if disclosure would be harmful to intergovernmental relations.

Part 2 of the *FOIP Act* allows for collection, use and disclosure of personal information for the purpose of law enforcement.

The *Act* also contains a provision that *requires* disclosure, without delay, of information about a risk of significant harm to the health or safety of the public, or information about a matter of compelling public interest.

Questions

14. Does the *FOIP Act* provide adequate protection against the disclosure of sensitive information that is requested through the access to information process? If not, please explain why and make suggestions for improvement.
15. Are there any cases where public bodies need broader powers to collect, use or disclose personal information in the interests of public security? If so, please identify these cases.

THE INDEPENDENT REVIEW

Another fundamental principle of the *Act* provides for independent oversight by an Information and Privacy Commissioner (**Part 4**). The Commissioner has a broad range of powers under the *Act*. These include the power to conduct investigations to ensure compliance with the *Act* or compliance with rules concerning the destruction of records, the power to delegate any of the Commissioner's powers, duties or functions under the *Act* to any person, except the power to delegate, to inform the public about the *Act* and to engage in research. As well, the Commissioner has the power to investigate and attempt to resolve complaints that a public body did not fulfil its duty to assist an applicant, or to determine that a fee is inappropriate and so on (**section 53**).

The Commissioner may also give advice and recommendations to heads of public bodies on matters concerning the *Act* (**section 54**).

The Commissioner has the power to authorize a public body to disregard requests (**section 55**) and has broad powers in conducting investigations (**section 56**).

The Commissioner may be asked to review a decision of a head by:

- an applicant in connection with any decision, act or failure to act by the head of a public body; and
- a third party that has been notified of an access request, in connection with a decision made by the head to disclose that third party's personal information or business information.

An applicant has 60 days from receiving the decision of the head to request a review by the Commissioner. A third party must request the review within 20 days of being advised of the decision. The request must be in writing. Detailed rules are provided in **Part 5** of the *Act* to regulate the conduct of a review. On completion of a review, a written order is made by the Commissioner and sent to the person requesting the review, to the public body and any other identified affected party. A Commissioner's Order is final and binding.

The Commissioner is also responsible for investigating alleged breaches of privacy by public bodies.

Questions

16. Are the powers and responsibilities of the Commissioner appropriate? If not, please explain why and provide suggestions for improvement.
17. Is the process established by the *Act* for the Commissioner to review decisions of public bodies appropriate? If not, please explain why and provide suggestions for improvement.

ADMINISTRATION OF THE ACT

The *Act* is administered by the Minister of Government Services, whose staff provide publications, training and support to public bodies. The Minister is also required to provide a directory of records (**section 87**) and an annual report on the operations of the *Act* (**section 86**).

Within public bodies, the head is accountable for performing the duties related to both access and privacy. Duties may be delegated to other officials (**section 85**). Public bodies have appointed FOIP Coordinators to manage the access and privacy process. These Coordinators serve as the primary contact point for the public.

Questions

18. Do you have any suggestions regarding the administration of the *Act*?
19. Now that local public bodies have been administering the *Act* for several years, are there any adjustments that could be made to the *Act* to improve its administration in a particular sector? Please explain.

FURTHER INFORMATION

If you require further information about the *Act* in order to prepare your submission, contact:

- the Queen's Printer Bookstores for purchasing a copy of the consolidated *Act* and *Regulation* (Edmonton – 780-427-4952; Calgary – 403-297-6251) or you can view the *Act* on the Queen's Printer web site at www.gov.ab.ca/qp.

- Alberta Government Services, Information Management, Access and Privacy for a Guide to the *Act* and other information (780-422-2657 or at www3.gov.ab.ca/foip).

- The Office of the Information and Privacy Commissioner for information about the role of that office (780-422-6860 or at www.oipc.ab.ca).

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT REVIEW – QUESTIONNAIRE

The personal information on this questionnaire, including your opinions, is collected under the authority of section 33(c) of the *Freedom of Information and Protection of Privacy (FOIP) Act* for consideration in the deliberations of the Select Special FOIP Act Review Committee and for preparing its Report. The Report will include the names of respondents and all respondents will receive a copy of the published Report. The submissions will be available to the public in the Legislature Library. If you have any questions about this collection, please contact the FOIP Coordinator of the Legislative Assembly Office, 9th Floor, Legislature Annex, 9718 – 107 Street, Edmonton, Alberta, T5K 1E4, Tel: (780) 427-1566.

Name: _____

Position Title:
(if applicable) _____

Organization:
(if applicable) _____

Address: _____

Phone: _____ Fax: _____

E-mail: _____

Signature: _____

1. Are the fundamental principles of the legislation appropriate? If not, please explain why and make suggestions for improvement.

_____

_____

_____

_____

2. Are the current criteria (structural approach) for including organizations within the scope of the *Act* appropriate? Do these criteria provide the flexibility needed for changing organizational structures or models (e.g. public-private partnerships or shared service arrangements)?

3. Are there any cases where excluded records or information should continue to be excluded from the access provisions of the *Act* (**Part 1**) but made subject to the *Act's* privacy provisions (**Part 2**)? Please specify which records or information and explain why this would be an improvement.

4. Are there any cases where a separate scheme of access and privacy for records or information that are not subject to the *FOIP Act* unreasonably limits access to records or the protection of personal information? Please specify which records or information and suggest how access or privacy protection might be improved.

5. Is the process for obtaining access to records appropriate? If not, please explain why and provide any suggestions for improvement.

6. Do you think that an applicant can locate the public body most able to respond to his or her request (e.g. by accessing the Government of Alberta web site and/or the FOIP web site, the Government's RITE Line, or by being referred by public body staff)?

7. Are the mandatory exceptions to disclosure appropriate? If not, please explain why and provide suggestions for improvement.

8. Are the discretionary exceptions to disclosure appropriate? If not, please explain why and provide suggestions for improvement.

9. Does the principle of sharing the costs between the public body and the applicant strike a fair balance between access rights and the responsibilities of public bodies to use their resources for program delivery? If not, explain why and make suggestions for improvement.

10. Is an appropriate balance struck between the interests of third parties and the rights of applicants? If not, please explain why and provide suggestions for improvement.

11. Is the definition of “personal information” in the *Act* appropriate? If not, please explain why and make suggestions for improvement.

12. Are the rules in the *Act* that control the manner in which public bodies collect, use and disclose personal information sufficient to protect the privacy and security of sensitive personal information? If not, please explain why and make suggestions for improvement.

13. Are there any issues associated with existing or emerging technologies that could be addressed through amendments to the *FOIP Act*? If so, please identify the issues.

14. Does the *FOIP Act* provide adequate protection against the disclosure of sensitive information that is requested through the access to information process? If not, please explain why and make suggestions for improvement.

15. Are there any cases where public bodies need broader powers to collect, use or disclose personal information in the interests of public security? If so, please identify these cases.

16. Are the powers and responsibilities of the Commissioner appropriate? If not, please explain why and provide suggestions for improvement.

17. Is the process established by the *Act* for the Commissioner to review decisions of public bodies appropriate? If not, please explain why and provide suggestions for improvement.

18. Do you have any suggestions regarding the administration of the *Act*?

19. Now that local public bodies have been administering the *Act* for several years, are there any adjustments that could be made to the *Act* to improve its administration in a particular sector? Please explain.

Please send your comments to:

Corinne Dacyshyn, Committee Clerk
Legislative Assembly of Alberta
801 Legislature Annex
9718 – 107 Street
Edmonton, Alberta T5K 1E4
FAX: (780) 427-5688
TEL: (780) 427-1348
e-mail: corinne.dacyshyn@assembly.ab.ca